Testimony of Carol Ashley

for the

House Subcommittee on National Security,
Emerging Threats, and International Relations Hearing

on

9/11 Commission Recommendations: Balancing Civil Liberties and Security

Washington, D.C.

June 6, 2006

DEFENDING AMERICA

On Memorial Day, a veteran remarked that we must defend freedom, or we will lose it. Defense of freedom is not only a function of our military. It is also a function of our Constitution and the laws which support it. You, the members of Congress, determine America's level of protection from both external and internal threats through your legislative decisions and oversight.

My name is Carol Ashley. I appreciate having the opportunity to appear before this subcommittee.

Before September 11th, like many other Americans, I assumed America was safe. That trust was shattered on 9/11 when my 25 year old daughter, Janice, was killed by terrorists at the World Trade Center. Although the government's foremost obligation is to protect us, something had gone horribly wrong. Our security network had failed.

Along with other 9/11 family members, I came to Washington, first seeking your help to establish an independent commission to investigate the attacks and later to press for passage of 9/11 legislation to improve security. Today I offer testimony in support of full implementation of the 9/11 Commission recommendations as they were envisioned, particularly strengthening the Privacy and Civil Liberties Oversight Board.

In light of the controversy over warrantless spying and the National Security Agency's (NSA's) amassing of phone records of millions of Americans, *The 9/11 Commission Report* seems prescient when it addressed privacy and civil liberty concerns.

> *"This shift of power and authority to the government calls for an enhanced system of checks and balances to protect the precious liberties that are vital to our way of life...*
>
> *"We must find ways of reconciling security with liberty since the success of one helps protect the other….[I]f our liberties are curtailed, we lose the values that we are struggling to defend."* [1]

Concerned that there was no federal office charged specifically with looking across the government to ensure that liberties are protected while the government gathers and shares intelligence, the Commission recommended that

> *"At this time of increased and consolidated government authority, there should be a board within the executive branch to oversee adherence to the guidelines we recommend and the commitment the government makes to defend our civil liberties."* [2]

EAVESDROPPING, PRIVACY AND THE LAW SINCE 9/11

Since September 11th, the government has been rigorous in attempting to track terrorism. I strongly support the work of our intelligence community and appreciate their efforts to prevent another terrorist attack. But I feel equally as strongly that the rights and freedoms guaranteed by the Constitution must not be abridged in the name of security.

There must be a balance between security and the right to privacy. That balance can be successfully achieved if these conditions are met:

- **Data is collected and discarded according to civilian and military law;**
- **There is rigorous, systematic oversight by a strong, independent Privacy and Civil Liberties Oversight Board, by Congress and by the FISA Court to ensure that protocol has been followed; to verify the integrity of the mission; and to safeguard the rights of innocent Americans.**

In its effort to prevent further terrorism, the government has initiated a series of controversial programs. Among them:

OPERATION TIPS (TERRORISM INFORMATION AND PREVENTION SYSTEM)

The TIPs program, proposed by Attorney General John Ashcroft, was intended to be a " '*national system for reporting suspicious, and potentially terrorist-related activity' involving 'millions of American workers who, in the daily course of their work, are in a unique position to see potentially unusual or suspicious activity in public places*.'" [3]

TOTAL INFORMATION AWARENESS (TIA)

Since 2002, when the Pentagon's Defense Research Projects Agency (DARPA) proposed the Total Information Awareness (TIA) program of computerized surveillance, there have been concerns about how to balance security with the right to privacy. (Later the name was changed to "Terrorist Information Awareness" program.) TIA was described as a "*system [that] would gather information about individuals from widely varied sources, including telephone calling records, credit card charges, banking transactions, airline reservations, and biometric databases -- all without search warrants or prior notice.*" [4] [5]

With black bag designation, TIA's status is shielded from Congressional oversight.

JET BLUE

In September, 2003, it was reported that a defense contractor, Torch Concepts, had used millions of JetBlue passenger records to test a prototype data-mining system

designed to screen out terrorists. Torch Concepts is a subcontractor to SRS Technologies, a defense contractor for DARPA's Information Awareness Office. The goal of the Torch system was to prevent terrorism by looking for behavioral and relationship patterns that would identify terrorist threats before a catastrophic attack could occur.

That mission is critically important and must be ongoing.

In the Torch project, private data was merged with JetBlue passenger information, including Social Security numbers, income, family members and the vehicles owned, to create a profile. David Neeleman, founder and CEO of JetBlue said he believed the data had been destroyed. [6] [7]

But was the data destroyed after the prototype testing was completed? There is no independent authority to verify that it was.

America needs a mechanism, answerable to Congress, for assessing sensitive programs that involve surveillance of Americans.

Unfortunately, Congressional oversight is hamstrung because the top line of the intelligence budget has not been declassified. Declassification would enable committees other than defense to have jurisdiction. Congress is urged to declassify the aggregate total of money appropriated for intelligence in the budget so that Congress can reorganize swiftly to fulfill its oversight obligations. That provision is in H.R. 5017.

THE PATRIOT ACT

When the Patriot Act passed on September 18th, 2001, it expanded the powers and surveillance options of the government. The Act relaxed controls over surveillance programs, eliminating the need for probable cause and decreasing judicial review. This concerned critics, who worried that fewer restraints would allow clandestine programs to infringe on citizens' rights and privacy. [8]

Earlier this year when the Patriot Act was amended and reauthorized, oversight provisions were added which required the Justice Department to monitor how often the FBI uses the powers and under what circumstances. Additionally, the law requires the administration to provide this information to Congress by certain dates. The oversight requirement was a positive step.

However, the President issued a "signing agreement"— an official document in which he gave his interpretation of the law. The President indicated that he is not obliged to obey the requirements to inform Congress if he determines that disclosure would ''*impair foreign relations, national security, the deliberative process of the executive, or the performance of the executive's constitutional duties*." [9]

How can the President's signing agreement which overrides a law established by the legislative branch, be reconciled with the balance of power envisioned by our founding fathers?

Congress is urged to quickly and aggressively regain its authority in the balance of power.

WARRANTLESS EAVESDROPPING

The NSA and other intelligence agencies are charged with gathering actionable intelligence about al Qaeda and other terrorist groups. The scope is international as well as domestic. All components of our intelligence apparatus must have the tools and latitude to do their job. Of necessity, their work is clandestine. Those who are working so hard to defend and protect this country should not be put in a position where they are ordered to violate the Constitutionally protected rights of Americans who pose no threat.

Although the White House initially insisted that NSA surveillance only involved calls overseas, this warrantless surveillance also included anti-war and environmental activists with no link to al Qaeda or terrorism. [10]

Surveillance of Activists

In December, 2005, NBC News and William M. Arkin, in his washingtonpost.com blog Early Warning, reported that TALON/CORNERSTONE, a Pentagon database, contained information on peace protesters and others whose activities posed no threat. [11] [12] [13]

Besides the NSA, the FBI, too, has apparently been spying without warrants. National Public Radio recently broadcast a segment called "Big Brother" which discussed an FBI program that spied on the environmental group, Greenpeace. It appears that the FBI relied heavily on information about Greenpeace provided by pro business, anti-regulation think tanks. A guest on the program, Ann Beeson, associate legal director of the ACLU, suggested that "*the FBI is not à [sic] just doing this to investigate crimes, but is doing it purposefully to suppress legitimate dissent and criticism of the administration's policies.*" [14]

The same questions apply to both the FBI and Pentagon surveillance of activists. What was the purpose of monitoring the activists? Who gave the order? Who received the surveillance reports, and as a result, what action was taken?

The danger posed by warrantless surveillance is its potential for abuse. These activists do not pose a terrorist threat. Americans have the right to peaceful dissent. In a democracy, dissent routs complacency, forcing attention on questionable government policies. It encourages people to learn more about the issues and ultimately, to express their support or displeasure to Congress and the White House. Oversight is needed to verify the integrity of mission of the surveillance — that it is legitimately for counterintelligence.

AT&T'S "SECRET ROOM"

Former AT&T technician Mark Klein alleges that AT&T cooperated in an illegal NSA domestic surveillance program. In 2003, AT&T, at the behest of the National Security Agency, built a "secret room" in its San Francisco office and possibly in other cities, where computer gear capable of spying on internet traffic was installed. This installation enabled the NSA to look at every message on the internet. [15]

NSA'S ACCESS TO PHONE RECORDS

It has been reported that the phone records of millions of Americans listing calls inside the US were turned over to the NSA by private phone companies. Two of the three phone companies named have subsequently denied the allegations. [16] [17] These records do not include names or addresses associated with the phone numbers, or the content of the calls. The records tell when calls were made and the duration. [18]

What is the truth of this story? Without oversight, there is simply no way of knowing.

USING PRIVATE DATA COLLECTORS

SKIRTING THE LAW?

The use of private contractors to collect personal data for surveillance programs is contentious.

> "*The agencies involved in data mining are trying to skirt the Privacy Act by claiming that they hold no data," said [Missouri Congressman William] Clay. Instead, they use private companies to maintain and sift through the data, he said.*
>
> *"Technically, that gets them out from under the Privacy Act," he said. "Ethically, it does not*." [19]

ONLINE DATA BROKERS

On May 25, TIME magazine reported that federal and local law enforcement may be circumventing privacy laws by obtaining calling records from online data brokers.

Some of these businesses obtain phone records illegally through "pretexting," in which someone who impersonates a subscriber inveigles the phone company to release copies of the records. Clients of some of these online brokers include an unnamed foreign government, the Department of Homeland Security (DHS) and the FBI. [20]

If the DHS and FBI are indeed buying information gathered by private data brokers with murky, possibly illegal authority, in addition to raising privacy concerns, the practice could jeopardize prosecution of terrorists and criminals.

SPIDER WEBS

Using phone records to develop spider webs is a useful tool in fighting terrorism. Constructing spider webs helps the NSA identify terrorists and operatives and contributes to clearer understanding of terrorist networks. A spider web is built by examining all calls to and from a specific phone number, then looking at calls to and from the numbers associated with the target number. [21]

In the Moussaoui case, perhaps the 9/11 plot would have been unraveled if the threads of a spider web had connected communication between Moussaoui and al Qaeda financiers and others in the terrorist network. We will never know. Inexplicably, FBI officials at headquarters repeatedly refused a Minnesota field agent's requests for a FISA warrant to access Moussaoui's belongings. Neither official has been held accountable. [22]

The danger of spider webs is that innocent people may be caught in the threads. To protect the innocent, and their rights, it is imperative that such surveillance is done within the parameters of the law. If our intelligence agencies indicate 72 hours is not long enough to apply for a FISA warrant, then it is Congress' responsibility to adjust the time frame, to ensure there is legal justification for abrogating a citizen's rights.

SECRECY — NECESSITY AND SHIELD

When government actions do not represent the ideals of our nation and who we are as a people, Americans need to know. Otherwise unworthy, unrepresentative actions persist. Exposure allows Americans to demand changes that reflect our ideals and our laws.

In surveillance programs such as those at the NSA which gather actionable intelligence, secrecy is integral to success. But secrecy can also be a tool to shield clandestine programs from inquiry and oversight.

Recently, attorneys in the Justice Department's Office of Professional Responsibility (OPR) were denied security clearance which halted their attempt to conduct an internal investigation into the Department's approval and oversight of the NSA's warrantless wiretapping program. The OPR was to determine whether Justice Department officials, including Attorney General Ashcroft and Attorney General Gonzales, acted properly in approving and overseeing the Bush administration's domestic eavesdropping program.

The classified documents which OPR attorneys wanted to access were those which had been given to Ashcroft, Gonzales and other Justice department attorneys involved in approving the NSA's warrantless eavesdropping in 2001. The Justice Department already has these documents, but the denial of clearance stopped the probe. It is not clear whether it was the NSA or the Attorney General who refused to grant clearance. [23]

In another instance involving the issue of security clearance, Russ Tice, a former intelligence officer with the NSA, has offered to testify before Congress about previously unreported spying by highly classified NSA and Defense Intelligence Agency Special Access Programs (SAPs). Tice was a specialist in space operations systems, command and control warfare, advanced technology and all-source collection analysis. [24] [25]

Tice was advised by Renee Seymour, director of NSA special access programs, that while he has the right to appear before Congress, he should not testify about the top secret electronic intelligence programs because *"neither the staff nor the members of the [House intelligence committee] or [Senate intelligence committee] are cleared to receive the information covered by the special access programs, or SAPs."* [26]

If no one except the NSA or DIA can be "read in" to receive clearance to investigate the surveillance programs, how can there ever be rigorous, independent oversight of programs that spy on Americans?

In an attempt to quash litigation over NSA warrantless eavesdropping, the Bush administration said that it would be impossible to defend the legality of NSA program without revealing classified information that would jeopardize national security. [27]

This poses a dilemma.

If the courts are prohibited from hearing cases involving possible illegal activity because of the need for secrecy, how can these surveillance programs be controlled?

The question of legality revolves around a presidential directive which overrode a 1978 FISA law requiring warrants for surveillance of American citizens. The President asserts that a congressional resolution passed after the terrorist attacks gave him the authority to order that warrantless eavesdropping, although a Congressional Research Service Report disagreed. [28] [29]

The status of balance of power and the use of states secrets designation to tip the scales in favor of the executive branch are underlying issues.

Although the matter of Presidential authority in the case of warrantless eavesdropping may ultimately be resolved in court, Congress must be vigilant to protect its position in the balance of power.

To safeguard our rights and prevent any one branch of government from exerting excessive power, Congress is urged to quickly and aggressively regain its authority in the balance of power.

No government agency or entity should have unfettered power to stop a legitimate, independent investigation into the legality of its work.

CONCLUSION

In the fight against terrorism, Americans must guard against incremental surrender of the freedoms which set us apart from repressive cultures. To protect our rights, surveillance inside our borders must be monitored to ensure compliance with the law. We depend on Congress to validate the legality, mission and integrity of our domestic surveillance programs.

But Congress has not fulfilled its oversight obligation regarding the nature and scope of clandestine surveillance. Congress has yet to resolve the issue of the legality of warrantless eavesdropping, the purpose behind the collection of phone records of millions of Americans, possible internet surveillance and whether other hidden programs are monitoring us. Secret domestic surveillance without legal boundaries, oversight or accountability is dangerous to a free society. There must be a balance between the need to gather actionable intelligence in the interest of national security and the right to privacy.

Secrecy, even that which falls legitimately under the aegis of national security, must not be allowed to trump America's system of checks and balances. Classifying previously unclassified documents, invoking states secrets without justification, and unfettered clandestine surveillance increase the potential for abuse, and with it the potential for insidious erosion of our rights to privacy and dissent. The freedoms we take for granted are at stake.

To counter the effects of secrecy and unfettered surveillance, these Congressional actions are recommended:

- **Declassify the top line of the intelligence budget so that Congress can reorganize itself for more effective oversight;**

- **Establish a strong truly independent Privacy and Civil Liberties Oversight Board as intended by the 9/11 Commission.**

Although the Commission recommended a strong, independent Civil Liberties Board with subpoena power, in 2004, Congress failed to follow that recommendation. It established instead a weak, ineffective board with no real authority. It has taken too long to become organized and its investigations can be nixed by the Attorney General. It is an oversight board in name only. As a result, America has government entities which are able to block legitimate inquiry, and over which there is no independent oversight.

Defending America from external and internal threats is paramount. There must be accountability for the legality and efficacy of the work being done. In defense of freedom, Congress must ensure that an independent agent looks across the government in its campaign against terror, to ensure that there is a balance between security and privacy.

- **Strengthen whistleblower protection for government workers, including those in the intelligence network.**

The Supreme Court decision of May 30, 2006, denying government whistleblowers first amendment protection will likely have a chilling effect on disclosure of agency misconduct, resulting in less government accountability.[30]

When a government worker has the courage and moral fortitude to reveal government misconduct to the American people, he or she must be protected by law. Since the Supreme Court ruling diminished First Amendment protection for workers on the job, Congress must act quickly to strengthen whistleblower protection for government workers, and this time include those in the intelligence network.

- **Pass House bill H. R. 5017 which fully implements the 9/11 Commission recommendations.**

Today, our military is deployed overseas to disrupt the terrorist network and destroy its training camps and sanctuary. But here at home we are not as well protected as we should be. The government has made progress and we are safer, but nearly 5 years after September 11th, serious internal security issues remain.

Airline cargo and ports are not secure, and neither are our borders. Thousands enter America illegally every month. Among them are people from countries rife with Islamic extremism. Although most illegal immigrants come to America seeking a better life, we must be very careful to monitor who enters our country. From experience we know that it takes only 19 savage Islamic extremists to murder thousands. Congress must act to secure our borders, closing the loopholes, literally and figuratively and provide adequate funding for hiring additional border control agents, increasing detention beds, and for implementing technology and physical barriers. Secure borders are critical to national security. [31] [32] [33]

All the provisions in this bill are important. Among those items which need immediate attention is to **mandate risk based funding**. Just this week, New York and Washington, D.C. were notified that their Homeland Security grant money had been slashed dramatically, even though they are probably the two most likely terrorist targets. New York was reduced from $207.5 million to $124.4 million and Washington from $77.5 million to $46.5 million. [34]

Strengthening nuclear counter proliferation as recommended by the 9/11 Commission is also a priority. Although attention is centered on Iran's capability to enrich uranium to weapons grade, focus should also be on the immediate danger posed by the availability of unsecured nuclear warheads and fissile material in the states comprising the former Union of Soviet Social Republics. [35]
Accessibility to this nuclear material, coupled with inadequate port security could have catastrophic consequences. The provisions in H. R. 5017 should be vigorously supported by Congress.

With your guidance, America can fulfill its national security obligations and simultaneously preserve the rights and freedoms that distinguish America.
Fully implementing the 9/11 Commission recommendations will reassure America that Congress is doing everything in its power to protect us from both foreign and domestic threats. It will begin to restore trust.

REFERENCES

[1] ***The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States***. W.W. Norton & Company, New York. 2004. 394-395

[2] Id., 395.

[3] Eggen, Dan, "Ashcroft: TIPS Plan Won't Have Central Database. " *The Washington Post.* July 26, 2002; Page A10. *http://www.washingtonpost.com/ac2/wp-dyn/A63340-2002Jul25?language=printer*

[4] Glass, Brett. "Security Alert: US Admiral Proposes "Big Brother" System." November 14, 2002. *http://www.extremetech.com/print_article2/0,1217,a=33650,00.asp*

[5] "Poindexter to resign over terror market flap." The Associated Press. *The Atlanta Journal-Constitution*. July 31, 2003. *http://www.realnews247.com/poindexter_to_quit_pentagon_post_amid_controversy.htm*

[6] Shachtman, Noah and Ryan Singel. "Army Admits Using JetBlue Data." September 23, 2003. *http://www.wired.com/news/business/0,60540-0.html*

[7] "JetBlue: Complaint for Violations of CA Business and Professions Code Sections 17200, et seq." *Privacy Rights Clearing House*. Posted September, 2003. *http://www.privacyrights.org/ar/jetbluecase.htm*

[8] Herman, Susan. "The USA Patriot Act and the US Department of Justice: Losing Our Balances?" December 3, 2001. *http://jurist.law.pitt.edu/forum/forumnew40.htm*

[9] Savage, Charlie. "Bush shuns Patriot Act requirement." *The Boston Globe*. March 24, 2006. *http://www.boston.com/news/nation/washington/articles/2006/03/24/bush_shuns_patriot_act_requirement/*

[10] Isikoff, Michael. "The Other Big Brother." *Newsweek*. Jan. 30, 2006. *http://www.msnbc.msn.com/id/10965509/site/newsweek*

[11] Pincus, Walter. "Pentagon Will Review Database on U.S. Citizens." *The Washington Post*. December 15, 2005; A01. *http://www.washingtonpost.com/wp-dyn/content/article/2005/12/14/AR2005121402528_pf.html*

[12] Arkin, William. "No Big Deal, Pentagon Says." February 9, 2006. *http://blogs.washingtonpost.com/earlywarning/2006/02/no_big_deal_pen.html#more*

[13] "Pentagon admits errors in spying on protesters." MSNBC and NBC News. March 10, 2006. *http://www.msnbc.msn.com/id/11751418*

[14] Berkowitz, Bill. “Green for Danger? “Feb 2, 2006.
http://www.ipsnews.net/print.asp?idnews=32013

[15] “Whistle-Blower's Evidence, Uncut.” May 22, 2006.
http://www.wired.com/news/technology/0,70944-0.html

[16] Cauley, Leslie. “NSA has massive database of Americans' phone calls.” *USA TODAY*. May 11, 2006.
http://www.usatoday.com/news/washington/2006-05-10-nsa_x.htm

[17] “Second Phone Company Questions 'USA Today' NSA Story.”
Editor and Publisher. May 16, 2006.
http://www.editorandpublisher.com/eandp/news/article_display.jsp?vnu_content_id=1002503697

[18] Hosenball, Mark and Evan Thomas. “Hold the Phone.” *Newsweek*.
May 22, 2006 issue. http://www.msnbc.msn.com/id/12779087/site/newsweek/

[19] Thompson, Doug. “NSA just one of many federal agencies spying on Americans.” *Capitol Hill Blue*. Dec 27, 2005.
http://www.capitolhillblue.com/artman/publish/printer_7904.shtml

[20] Dell, Kristina. “Are the Police Digging into Your Phone Records?” *TIME*. May. 25, 2008 [sic] (Actual date of posting, May 25, 2006.)
http://www.time.com/time/nation/printout/0,8816,1197918,00.html

[21] Diamond, John and David Jackson. “Bush says privacy protected; sources tell of 'spider web' use.” *USA Today*. May 12, 2006.
http://www.usatoday.com/news/washington/2006-05-11-nsa-database-furor_x.htm

[22] Sniffen, Michael J. “FBI Agent Slams Bosses at Moussaoui Trial.” Associated Press. March 20, 2006.
http://news.yahoo.com/s/ap/20060320/ap_on_re_us/moussaoui_11&printer=1;_ylt=AvWvbI3LErxmwZz.bkk0_ehH2ocA;_ylu=X3oDMTA3MXN1bHE0BHNlYwN0bWE-

[23] Harris, Shane and Murray Waas. “Investigators denied clearances for probe of eavesdropping program.” *National Journal*. May 26, 2006.
http://www.govexec.com/dailyfed/0506/052606nj1.htm

[24] Gertz, Bill. “NSA whistleblower asks to testify.” *THE WASHINGTON TIMES*. January 5, 2006.
http://www.washtimes.com/national/20060104-114052-6606r.htm

[25] Strohm, Chris. “Former NSA officer alleges illegal activities under Hayden.” *CongressDaily*. May 12, 2006.
http://www.govexec.com/story_page.cfm?articleid=34075

[26] Gertz, Bill. “Ex-official warned against testifying on NSA programs.” *THE WASHINGTON TIMES*. January 12, 2006.
http://www.washingtontimes.com/national/20060111-112622-2876r.htm

[27] Caruso, David B. "Dismissal of Lawsuits Over NSA Eavesdropping Sought." Associated Press. *The Washington Post*. May 28, 2006; A13
http://www.washingtonpost.com/wp-dyn/content/article/2006/05/27/AR2006052700819_pf.html

[28] Id.

[29] Leonnig, Carol D. "Report Rebuts Bush on Spying." *The Washington Post*. January 7, 2006; A01.
http://www.washingtonpost.com/wp-dyn/content/article/2006/01/06/AR2006010601772_pf.html

[30] "Court curbs government whistleblowers." Associated Press. May 30, 2006. *http://www.msnbc.msn.com/id/13047151/from/RSS/*

[31] Malkin, Michelle. "What's the Spanish Word for 'Terrorist'?" July 24, 2004. *http://michellemalkin.com/archives/000275.htm*

[32] "Potential terrorists released due to lack of jail space, congressman says," Emma Perez-Trevino. *The Brownsville Herald.* July 23, 2004.
http://www.brownsvilleherald.com/ts_comments.php?id=60297_0_10_0_C

[33] Seper, Jerry. "Guarding America's Border." THE WASHINGTON TIMES. December 8, 2003
http://washingtontimes.com/national/20031208-123627-3333r.htm

[34] Newman, Maria. "To Some Mayors, Security Grants Seemed Fair ." *The New York Times*. June 1, 2006.
http://www.nytimes.com/2006/06/01/washington/01cnd-homeland.html?hp&ex=1149220800&en=3c8507366b1afb32&ei=5094&partner=homepage

[35] "Open ports, loose nukes," Globe Editorial. *The Boston Globe*. February 28, 2006.
http://www.boston.com/news/globe/editorial_opinion/editorials/articles/2006/02/28/open_ports_loose_nukes /